UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/631,989	07/31/2003	Bjorn Markus Jakobsson	4414-34	2203

7590   04/18/2007

Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560

EXAMINER
TESLOVICH, TAMARA

ART UNIT	PAPER NUMBER
2137	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/18/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

PTOL-90A (Rev. 10/06)

		Application No.	Applicant(s)
		10/631,989	JAKOBSSON ET AL.
Office Action Summary		Examiner	Art Unit
		Tamara Teslovich	2137

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>*31 July 2003*</u>.

2a)☐ This action is **FINAL.**   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>*11/13/03*</u> is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date <u>*08.25.03*</u>.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application

6)☐ Other: _____ .

DETAILED ACTION

This Office Action is in response to the Application for Patent filed on July 31, 2003.

Claims 1-30 are pending are herein considered.

Claim Objections

Claims 1-30 are objected to for failing to positively recite claim limitations. The subject matter of a properly construed claim is defined by the terms that limit its scope. As a general matter, the grammar and intended meaning of terms used in a claim will dictate whether the language limits the claim scope. Language that suggests or makes optional but does not require steps to be performed or does not limit a claim to a particular structure does not limit the scope of a claim or claim limitation. The following are examples of language that may raise a question as to the limiting effect of the language in a claim:

(A) statements of intended use or field of use,

(B) "adapted to" or "adapted for" clauses,

(C) "wherein" clauses, or

(D) "whereby" clauses.

This list of examples is not intended to be exhaustive. See also MPEP § 2111.04.

Claims are to be given their broadest reasonable interpretation in light of supporting disclosure. In re Morris, 127 F.3d 1048, 1054-55, 44 USPQ2d 1023, 1027-28 (Fed. Cir. 1997). Limitations appearing in the specification but not recited in the claim

should not be read into the claim. E-Pass Techs., Inc. v. 3Com Corp., 343 F.3d 1364,

1369, 67 USPQ2d 1947, 1950 (Fed. Cir. 2003) (claims must be interpreted "in view of

the specification" without importing limitations from the specification into the claims

unnecessarily). In re Prater, 415 F.2d 1393, 1404-05, 162 USPQ 541, 550-551 (CCPA

1969). See also In re Zletz, 893 F.2d 319, 321-22, 13 USPQ2d 1320, 1322 (Fed. Cir.

1989) ("During patent examination the pending claims must be interpreted as broadly as

their terms reasonably allow.... The reason is simply that during patent prosecution

when claims can be amended, ambiguities should be recognized, scope and breadth of

language explored, and clarification imposed.... An essential purpose of patent

examination is to fashion claims that are precise, clear, correct, and unambiguous. Only

in this way can uncertainties of claim scope be removed, as much as possible, during

the administrative process.").

Those phrases objected to by the Examiner include but are not limited to "such

that", "so as to permit", "being configurable to/for", "being utilizable" and "being operative

to"

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by
another filed in the United States before the invention by the applicant for patent or (2) a patent
granted on an application for patent by another filed in the United States before the invention by the
applicant for patent, except that an international application filed under the treaty defined in section
351(a) shall have the effects for purposes of this subsection of an application filed in the United States

only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-30 are rejected under 35 U.S.C. 102(e) as being anticipated by United

States Patent No. 7,082,604 B2 to Marc Schneiderman.

As per claim 1, Schneiderman teaches a method for partitioning of cryptographic functionality so as to permit delegation of at least one of a plurality of distinct portions of the cryptographic functionality from a delegating device to at least one recipient device, the cryptographic functionality being characterizable as a graph comprising a plurality of nodes (Figures 24-25, col.1 lines 10-31, col.3 lines 49-67), the method comprising the steps of: associating a given set of the nodes with a corresponding one of the plurality of distinct portions of the cryptographic functionality; and transmitting from the delegating device to the recipient device information representative of one or more of the nodes, such that the recipient device is thereby configurable for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality (col.21 lines 54-67; col.22 lines 10-48).

As per claim 2, Schneiderman teaches wherein at least one of the nodes of the graph corresponds to a seed the possession of which permits execution of a corresponding one of the distinct portions of the cryptographic functionality (col.21 lines 54-67).

As per claim 3, Schneiderman teaches wherein the transmitting step further comprises transmitting from the delegating device to the recipient device information representative of at least two of the nodes (col.24 lines 28-55).

As per claim 4, Schneiderman teaches wherein the transmitting step further comprises transmitting from the delegating device to the recipient device information

representative of at least one parent node of the graph (Figures 24-25, col.1 lines 10-31, col.3 lines 49-67).

As per claim 5, Schneiderman teaches wherein the transmitting step further comprises transmitting from the delegating device to the recipient device information representative of at least one child node of a parent node of the graph (Figures 24-25, col.1 lines 10-31, col.3 lines 49-67).

As per claim 6, Schneiderman teaches wherein the graph comprises at least first and second root nodes (Figures 24-25, col.1 lines 10-31, col.3 lines 49-67).

As per claim 7, Schneiderman teaches wherein the graph comprises a tree having at least first and second subtrees associated with respective first and second ones of the plurality of distinct portions of the cryptographic functionality (Figures 24-25, col.1 lines 10-31, col.3 lines 49-67).

As per claim 8, Schneiderman teaches wherein the graph comprises a chain (Figures 24-25, col.1 lines 10-31, col.3 lines 49-67).

As per claim 9, Schneiderman teaches wherein the graph comprises L levels of nodes, an Lth one of the levels comprising a parent node $v.sub.L,1$, and a first one of these levels comprising a set of seeds $v.sub.1,1$, $v.sub.1,2$, . . . $v.sub.1,n$, where n is the total number of seeds, each of the seeds being derivable from the parent node (Figures 24-25, col.1 lines 10-31, col.3 lines 49-67).

As per claim 10, Schneiderman teaches wherein an ith node of a kth one of the levels is computed as $f.sub.k(i, v.sub.k+1)$, where $f.sub.k$ is a one-way function (Figures 24-25, col.1 lines 10-31, col.3 lines 49-67).

As per claim 11, Schneiderman teaches wherein the nodes of one or more of the levels are arranged in the form of tuples of designated numbers of nodes (Figures 24-25, col.1 lines 10-31, col.3 lines 49-67).

As per claim 12, Schneiderman teaches wherein the ith node of a jth tuple of the kth level is computed as f.sub.k(j, i, v.sub.k+1,j) (Figures 24-25, col.1 lines 10-31, col.3 lines 49-67).

As per claim 13, Schneiderman teaches wherein the cryptographic functionality comprises a cryptographic functionality provided by a hardware-based authentication token (col.3 lines 7-39).

As per claim 14, Schneiderman teaches wherein the cryptographic functionality comprises an ability to verify at least one of an authentication code and a distress code generated by a hardware-based authentication token (col.3 lines 7-39).

As per claim 15, Schneiderman teaches wherein the authentication token is configured to store at least two seeds, and the cryptographic functionality comprises a verification operation performed collaboratively by at least first and second servers each storing one of the seeds (col.3 lines 40-67).

As per claim 16, Schneiderman teaches wherein the cryptographic functionality comprises an ability to generate at least one of an authentication code and a distress code utilizing a hardware-based authentication token (col.3 lines 40-67).

As per claim 17, Schneiderman teaches wherein the cryptographic functionality comprises at least one of an ability to verify a signature and an ability to generate a signature (col.3 lines 7-39).

As per claim 18, Schneiderman teaches wherein the cryptographic functionality comprises an ability to generate one or more values of a one-way chain (col.3 lines 7-39).

As per claim 19, Schneiderman teaches wherein the cryptographic functionality comprises an ability to perform symmetric cryptographic operations (col.5 lines 48-63).

As per claim 20, Schneiderman teaches wherein the cryptographic functionality comprises an ability to perform asymmetric cryptographic operations (col.22 lines 49-67).

As per claim 21, Schneiderman teaches wherein the cryptographic functionality comprises an ability to derive one or more cryptographic keys (col.5 lines 48-63).

As per claim 22, Schneiderman teaches wherein the cryptographic functionality comprises an ability to compute one or more seeds (col.5 lines 48-63).

As per claim 23, Schneiderman teaches wherein at least one of the seeds corresponds to at least one of the nodes of the graph (col.5 lines 48-63).

As per claim 24, Schneiderman teaches wherein the cryptographic functionality is partitioned in accordance with a subscription model which requires compliance with at least one specified criterion for transmission from the delegating device to the recipient device of the information representative of one or more of the nodes (col.24 lines 14-28).

As per claim 25, Schneiderman teaches wherein compliance with the specified criterion is satisfied upon receipt of a designated payment (col.14 lines 35-46).

As per claim 26, Schneiderman teaches wherein the recipient device and the delegating device collaborate to perform at least one of a cryptographic verification function and a cryptographic generation function (col.14 lines 47-67).

As per claim 27, Schneiderman teaches wherein the recipient device includes only a limited computational ability associated with performance of the cryptographic function (col.16 lines 18-41).

As per claim 28, Schneiderman teaches an apparatus comprising: a processing device comprising a processor coupled to a memory; the processing device being utilizable in conjunction with partitioning of cryptographic functionality so as to permit delegation of at least one of a plurality of distinct portions of the cryptographic functionality from the processing device, configured as a delegating device, to at least one recipient device, the cryptographic functionality being characterizable as a graph comprising a plurality of nodes (Figures 24-25, col.1 lines 10-31, col.3 lines 49-67); the processing device being configurable to associate a given set of the nodes with a corresponding one of the plurality of distinct portions of the cryptographic functionality, and to transmit to the recipient device information representative of one or more of the nodes, such that the recipient device is thereby configurable for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality (Figures 24-25, col.1 lines 10-31, col.3 lines 49-67).

As per claim 29, Schneiderman teaches an apparatus comprising: a processing device comprising a processor coupled to a memory; the processing device being utilizable in conjunction with partitioning of cryptographic functionality so as to permit

delegation of at least one of a plurality of distinct portions of the cryptographic

functionality to the processing device, configured as a recipient device, from at least one

delegating device, the cryptographic functionality being characterizable as a graph

comprising a plurality of nodes (Figures 24-25, col.1 lines 10-31, col.3 lines 49-67); a

given set of the nodes being associated with a corresponding one of the plurality of

distinct portions of the cryptographic functionality; the processing device being operative

to receive from the delegating device information representative of one or more of the

nodes, such that the processing device is thereby configurable for authorized execution

of a corresponding one of the plurality of distinct portions of the cryptographic

functionality (Figures 24-25, col.1 lines 10-31, col.3 lines 49-67).

As per claim 30, Schneiderman teaches a machine-readable storage medium

containing one or more software programs for use in partitioning of cryptographic

functionality so as to permit delegation of at least one of a plurality of distinct portions of

the cryptographic functionality from a delegating device to at least one recipient device,

the cryptographic functionality being characterizable as a graph comprising a plurality of

nodes (Figures 24-25, col.1 lines 10-31, col.3 lines 49-67), wherein the one or more

software programs when executed by the delegating device implement the steps of:

associating a given set of the nodes with a corresponding one of the plurality of distinct

portions of the cryptographic functionality; and transmitting from the delegating device to

the recipient device information representative of one or more of the nodes, such that

the recipient device is thereby configurable for authorized execution of a corresponding
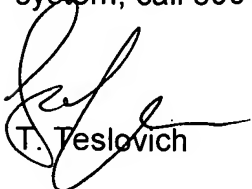
one of the plurality of distinct portions of the cryptographic functionality (Figures 24-25, col.1 lines 10-31, col.3 lines 49-67).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571) 272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

T. Teslovich

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137